METHOD AND APPARATUS FOR PROTECTING COPYRIGHT OF DIGITAL RECORDING MEDIUM AND COPYRIGHT PROTECTED DIGITAL RECORDING MEDIUM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a copyright protection for a digital recording medium, and more particularly, to a copyright protection method and apparatus for a digital recording medium storing encrypted data and a copyright protected digital recording medium.

2. Description of the Related Art

In the future as well as at present, a copyright protection for all contents or software used in audio/video (A/V) equipment or computer-related equipment is indispensable. Accordingly, hardware or software having various copyright protection functions are under development according to various standards or rules.

One of currently developed or proposed copyright protection techniques utilizes the principle of a cryptosystem. There are a symmetrical cryptosystem represented by a data encryption standard (DES) and an asymmetrical cryptosystem represented by an RSA (Riverst, Shamir & Adleman), as a cryptosystem for encrypting information or message itself. There are an authentication system and a content scramble system (CSS) as methods used to realize the above cryptosystem. There are a user authentication, a digital signature or a message authentication as the authentication system.

A macrovision being a widely spread copyright protection technique prevents a digital-to-analog copy. For example, when a copy or replica is attempted into analog magnetic tape as in a conventional video cassette recorder (VCR), the macrovision makes a sync signal continuously varied at random, to thus lower a picture quality abruptly. The content scramble system (CSS) being another copyright protection technique employs the authentication system and the cryptosystem at the same time, in order to prevent a digital-to-digital copy. The

CSS is used for copyright protection of a digital versatile disk (DVD) ROM drive and a DVD decrypter card mounted on a computer. After the DVD-ROM drive and the DVD decrypter card have authenticated each other, encrypted A/V data which is recorded on a DVD-ROM is decoded through the decrypter card. That is, the DVD-ROM drive uses an incorporated chip or program to perform an authentication work with respect to the DVD decrypter card, and the DVD decrypter card uses an incorporated chip or program to perform an authentication work and a data decoding operation.

Meanwhile, a DVD player includes a separate chip or a micro-controller program which can decrypt encrypted data, and reads and reproduces the encrypted A/V data from a DVD without having an authentication procedure.

Using the above-described copyright protection techniques can only prevent unauthorized copies of general users, but cannot prevent unauthorized copies of technical copying experts.

SUMMARY OF THE INVENTION

To solve the above problems, it is an object of the present invention to provide a copyright protection method for a digital recording medium storing encrypted data.

It is another object of the present invention to provide a digital recording medium whose copyright is protected.

It is still another object of the present invention to provide an apparatus using a digital recording medium whose copyright is protected.

To accomplish the above object of the present invention, there is provided a copyright protection method for protecting a copyright with respect to a digital recording medium, the copyright protection method comprising the steps of: (a) encrypting information to be recorded using a cryptosystem; (b) recording the information encrypted in step (a) on the digital recording medium; and (c) recording a cypher key necessary for decryption of the information encrypted in step (a) on the digital recording medium in a manner that the cypher key is not allowed to be copied.

There is also provided a digital recording medium comprising: a data recording

region on at least one part of which information encrypted using a cryptosystem is recorded; and a copy disapproval region on which a cypher key necessary for decryption of the encrypted information recorded on the data recording region is recorded.

There is further provided a playback apparatus for a digital recording medium including a data recording region on at least one part of which information encrypted using a cryptosystem is recorded; and a copy disapproval region on which a cypher key necessary for decryption of the encrypted information recorded on the data recording region is recorded, the playback apparatus comprising: a memory for storing the cryptosystem; a reader for reading data recorded on the digital recording medium; and a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

There is still further provided a digital recording and/or reproducing apparatus comprising: a digital recording medium including a data recording region on at least one part of which information encrypted using a cryptosystem is recorded and a copy disapproval region on which a cypher key necessary for decryption of the encrypted information recorded on the data recording region is recorded; a memory for storing the cryptosystem; a reader for reading data recorded on the digital recording medium; and a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

BRIEF DESCRIPTION OF THE DRAWINGS

The above objects and other advantages of the present invention will become more apparent by describing the preferred embodiment thereof in more detail with reference to the accompanying drawings in which:

FIG. 1 is a flowchart diagram for explaining a signal processing when data is recorded on a DVD-ROM;

FIG. 2 shows the structure of a BCA code;

FIG. 3 is a flowchart diagram for explaining a signal processing when data is

recorded on a DVD-ROM according to an embodiment of the present invention; and

FIG. 4 is a block diagram showing a digital recording/reproducing apparatus according to another embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the present invention will be described with reference to the accompanying drawings.

When encrypted data is recorded on a digital recording medium according to an embodiment of the present invention, a cypher key for decrypting the encrypted data is recorded on a copy disapproval region of the digital recording medium. Thus, a playback apparatus can reproduce encrypted data such as programs or information recorded on the digital recording medium only in the case that the cypher key recorded on the digital recording medium can be reproduced. In embodiments according to the present invention, after data has been encrypted using various cryptosystems including a symmetrical cryptosystem and an asymmetrical cryptosystem, the encrypted data is recorded on a data recording region of the digital recording medium and a cypher key used for encryption of data is recorded on a copy disapproval region positioned in the outer area of the data recording region. Here, the data recording region is comprised of a lead-in area, a user or data area, and a lead-out area, and the copy disapproval region is positioned in the outer area of the data recording region. In particular, in the case that the digital recording medium is an optical disk, the copy disapproval region is positioned in the outer area of the lead-in area and in a position where an optical head can read data recorded on the copy disapproval region.

Prior to describing a first embodiment of the present invention, a general data recording method with respect to a DVD-ROM will be described below with reference to FIG. 1.

When software such as Audio/Video (A/V) data or programs is recorded on a DVD-ROM, the data or program is signal-processed in units of main data of 2048 bytes obtained by dividing the data or program. In step 101, identification (ID) data of 4 bytes and an ID error detection code (IDE) of 2 bytes for the ID are added in

each main data. Then, copyright management information CPR_MAI of 6 bytes is added therein in step 102. An error detection code (EDC) for all the ID, IDE, CPR_MAI and the main data is added therein (step 103). After the EDC has been added, only the main data is scrambled (step 104). A data sector is produced performing steps 101 through 104.

An error correction (ECC) encoding for data sectors is performed with respect to 16 data sectors (step 105). A parity outer (PO) portion of 16 rows obtained by the ECC encoding is interleaved within the data sectors (step 106). As a result, 16 recording sectors are produced (step 107). Each recording sector is separated into 26 sync frames and data in each sync frame is eight-to-fourteen plus (EFM+) modulated using an EFM plus table (step 108). The EFM+ modulation is modified from EFM modulation data that is used for recording data on a compact disk (CD), in order to be appropriate for recording data on a read-only DVD (DVD-ROM). Actually, the EFM+ modulation is an eight-to-sixteen modulation for converting an 8-bit symbol into a 16-bit codeword expressed by a binary code. By performing step 108, 16 physical sectors are produced.

The EFM+ table used in step 108 complies with specifications for a DVD-ROM and is comprised of a main conversion table and a substitution table. Each of the main conversion table and the substitution table has four states. Each state has 16-bit codewords individually corresponding to symbols and next state values individually corresponding to the codewords. For reference, the main conversion table has an association relationship between the codewords corresponding to 256 symbols. Since each state has the codeword and the corresponding next state value, a digital sum variation (DSV) is as close as possible to a direct-current (DC) level. As a DSV is closer to a DC level, a stable signal characteristic is provided even in the case of eccentricity of a DVD-ROM or damage on the disk surface.

In this embodiment of the present invention, data to be recorded is modulated using a EFM+ table varied from the above-described EFM+ table, to thereby record the encrypted data on a recording medium. Also, in this embodiment, a table number representing a varied EFM+ table used for encrypting the data is used as a cypher key, and is recorded on a copy disapproval region of the recording medium,

in order to protect a copyright with respect to the recording medium storing the data. For clarity, an EFM+ table according to the specifications for a DVD-ROM is defined as a "fundamental EFM+ table", and a EFM+ table modified from the fundamental EFM+ table is defined as a "varied EFM+ table".

In order to vary a fundamental EFM+ table according to the specifications for a DVD-ROM within a range where an error does not occur in a DVD recording and/or reproducing apparatus, the embodiment of the present invention lets symbols corresponding to decimal numbers 0 through 255 in the above-described main conversion table shift by one place. For example, when the main conversion table includes a codeword "0010 0000 0000 1001" corresponding to a symbol value "0", a codeword "0010 0000 0001 0010" corresponding to a symbol value "1", and a codeword "0010 0001 0010 0000" corresponding to a symbol value "2", one of the varied main conversion table has a codeword "0010 0000 0001 0010" corresponding to a symbol value "0" and a codeword "0010 0001 0010 0000" corresponding to a symbol value "1". The above varying method of the fundamental EFM+ table, that is, a method for producing varied EFM+ tables by re-associating a symbol-codeword relationship in the fundamental EFM+ table is obvious to anyone who has an ordinary skill in the art. Therefore, the detailed realization method will be omitted.

When a main conversion table is varied in the above manner, 255 varied EFM+ tables are obtained from the fundamental EFM+ table. In this embodiment, a symbol value in the main conversion table is used as a table number for each EFM+ table, in order to discriminate a total of 256 EFM+ tables including a fundamental EFM+ table from each other. Therefore, a varied EFM+ table having a codeword corresponding to a symbol value "1" in the unvaried main conversion table as a codeword corresponding to its own symbol value "0", has a table number "1". Also, the fundamental EFM+ table having the unvaried main conversion table has a table number "0". Such table numbers can be expressed by one byte, and can be changed as any figure or can be included in a serial number designated on a disk by a manufacturer. The table number is necessary for decoding the corresponding software and thus is recorded on a copy disapproval region in the DVD-ROM.

In the following, a copy disapproval region in a DVD-ROM where a table

number corresponding to a varied EFM+ table used for modulating information to be recorded according to an embodiment of the present invention is recorded, will be described with reference to FIG. 2.

The DVD-ROM contains a burst cutting area (BCA) as a copy disapproval data recording region. A BCA code recorded on the BCA has a BCA preamble field of one row, a BCA data field composed of 4n (wherein $1 \leq n \leq 12$ and n is an integer), and a BCA postamble field of one row, in which each row has 5 bytes in size. These three BCA fields are sequentially recorded on a DVD without having a gap. The BCA preamble field has a BCA sync SB_{BCA} of one byte and a BCA preamble of 4 bytes following the SB_{BCA}. The BCA data field has a BCA re-sync RS_{BCA} being a leading portion of each row, a plurality of information data I_0, I_1, ..., I_{16n-5} and an error correction code ECC_{BCA}. Each of the information data and the error correction code has 4 bytes in size.

In a first embodiment of the present invention, the BCA preamble of the above-described BCA, particularly, the last byte in the BCA preamble is used for recording a table number. Therefore, the BCA preamble becomes "00h 00h 00h XXh" including "XXh" representing a table number of the varied EFM+ table used for modulating the information to be recorded. In the case that a fundamental EFM+ table defined in the specifications for a DVD-ROM is used for modulation of data, a BCA preamble becomes "00h 00h 00h 00h". Therefore, the present invention can be compatible with a DVD playback apparatus which does not support a varied EFM+ table.

FIG. 3 is a flowchart diagram for explaining a method for generating 16 physical sectors from data to be recorded, which is used in the first embodiment of the present invention.

In FIG. 3, steps 101 through 107 are the same as those described with reference to FIG. 1. Thus, the detailed description thereof will be omitted. In step 310, when encrypting data to be recorded, one of the 255 varied EFM+ tables excepting the fundamental EFM+ table is selected.

The 256 EFM+ tables are stored in a storage (not shown) in a DVD recording and/or reproducing apparatus and selectively used from the storage for EFM-

modulating data to be recorded and/or reproduced. The EFM+ tables are stored in the storage in the form of a variable EFM+ table which can generate the above-described 256 EFM+ tables by re-associating a symbol-codeword relationship. In this case, a varied EFM+ table which is obtained from the variable EFM+ table and corresponds to information to be recorded and/or reproduced is stored in a separate RAM and the varied EFM+ table stored in the separate RAM is used for modulating and/or demodulating information to be recorded and/or reproduced. By doing so, data can be demodulated at a desired speed. Alternatively, 256 EFM+ tables stored in a ROM are used. In step 320, information to be recorded is modulated using a selected varied EFM+ table. As a result, 16 physical sectors are produced.

However, if all data including information to be recorded on a DVD-ROM is modulated using a varied EFM+ table and then recorded on a DVD, there is a problem concerning a compatibility during playback of the DVD. Thus, data to be recorded on a lead-in area of the DVD is modulated using a fundamental EFM+ table and information to be recorded on an information recording area of the DVD is modulated using a varied EFM+ table.

In step 330, separate data representative of a varied EFM+ table used for recording information on a DVD-ROM, that is, a cypher key such as the above-described table number is recorded on a separate region on the DVD-ROM, i.e. a BCA preamble.

When reproducing the DVD-ROM, a DVD playback apparatus first reads a BCA code from the DVD-ROM to recognize a table number. Then, a demodulator in the DVD playback apparatus reads a varied EFM+ table corresponding to the recognized table number from an internal table RAM and demodulates information recorded on the DVD-ROM, for example, A/V data or programs.

The above-described embodiment can be easily applied to A/V equipment or computer-related equipment which is essentially inexpensive, differently from the equipment using existing copyright protection techniques requiring separate hardware or software and a common standard.

The above-described first embodiment of the present invention uses a recording modulation of data using an EFM+ table as a cryptosystem. However,

the present invention is not limited to the above embodiment. Therefore, the present invention can be applied to a digital recording medium storing encrypted data using various cryptosystems and various digital recording and/or reproducing systems for the digital recording media.

FIG. 4 shows a digital recording and/or reproducing apparatus according to a second embodiment of the present invention. The apparatus shown in FIG. 4 uses an existing recording modulation method for a data recording modulation without any modification, and uses a separate cryptosystem for encrypting information to be recorded and/or decrypting the encrypted information to be reproduced.

The apparatus of FIG. 4 performs recording and/or reproduction of the encrypted information with respect to an optical disk 41. The apparatus includes a recorder/reader 43 for the optical disk 41, a memory 45 for storing the cryptosystem and an encryptor/decryptor 47 for encrypting or decrypting information using the cryptosystem stored in the memory 45.

The optical disk 41 includes a data recording region for recording the encrypted information and a BCA used as a copy disapproval region. Recorded on the BCA is a cypher key for decrypting the encrypted information recorded on the data recording region. A portion on which the cypher key is recorded is a BCA preamble. However, since the recording position does not limit the present invention, the cypher key can be recorded on a portion where an undefined portion exists in the BCA data field. The BCA is formed on a portion of a transparent window located between a central hole and a lead-in region on the optical disk. In particular, the BCA is formed on a position where an optical head provided in the recorder/reader 43 can read data recorded on the BCA. A DVD-ROM, a DVD-RAM or a hybrid DVD can be used as the optical disk 41 used in the FIG. 4 apparatus. The hybrid DVD has a read-only ROM area and a rewritable RAM area as the data recording region.

When the FIG. 4 apparatus reproduces the optical disk 41 containing encrypted information, the recorder/reader 43 reads a cypher key recorded on the BCA of the optical disk 41 loaded into a deck (not shown) and reads the encrypted information recorded on the data recording region. The encrypted information and the cypher

key are supplied to the encryptor/decrypter 47. The encryptor/decrypter 47 decrypts the encrypted information using the read cypher key and the cryptosystem stored in the memory 45. The decrypted information is supplied to a signal processor (not shown).

The encrypted information recorded on the data recording region of the optical disk 41 can be encrypted using existing various encryption systems or techniques. Therefore, in the case that the memory 45 stores cryptosystems according to a plurality of encryption techniques, the FIG. 4 apparatus can decrypts the data stored on the optical disk 41 and encrypted using the various cryptosystems, by means of a corresponding cryptosystem stored in the memory 45 and a single cypher key recorded on the BCA. Also, when the memory 45 is implemented as a RAM, the cryptosystem recorded in the memory 45 can be altered into another cryptosystem.

Meanwhile, the optical disk 41 is a DVD-RAM or a hybrid DVD which is legally sold or provided, the FIG. 4 apparatus encrypts new information using the cypher key which has been already recorded on the BCA and records the encrypted new information on the optical disk 41, or records the encrypted information which can be decoded using the cypher key recorded on the BCA, on the optical disk 41. Therefore, in this case, a software provider can provide encrypted information to be added in the contents contained in the optical disk 41 only to a legal end user, without any separate confirmation on whether the optical disk 41 is possessed legally.

In the above second embodiment, a recording and reproducing apparatus for a digital recording medium has been described. However, it is also obvious to anyone skilled in the art that a reproduction-only apparatus for a digital recording medium can be embodied from the second embodiment within the scope of the present invention.

As described above, the copyright protection method and apparatus and the copyright protected digital recording medium can protect a copyright with respect to contents which are sold or provided by means of digital recording media. In addition, since a copyright protection function can be realized using a currently available modulation table, a playback apparatus for a copyright protected digital

recording medium can be manufactured at low cost.

What is claimed is:

1. A copyright protection method for protecting a copyright with respect to a digital recording medium, the copyright protection method comprising the steps of:

(a) encrypting information to be recorded using a cryptosystem;

(b) recording the information encrypted in step (a) on the digital recording medium; and

(c) recording a cypher key for decrypting the information encrypted in step (a) on the digital recording medium in a manner that the cypher key is not allowed to be copied.

2. The copyright protection method according to claim 1, wherein said digital recording medium is an optical disk and said cypher key is recorded on a burst cutting area (BCA).

3. The copyright protection method according to claim 2, wherein said cypher key is recorded on a BCA preamble.

4. The copyright protection method according to claim 2, wherein said optical disk is a digital versatile disk (DVD) and said cryptosystem is a content scramble system.

5. The copyright protection method according to claim 2, wherein said optical disk is a DVD-ROM.

6. The copyright protection method according to claim 2, wherein said optical disk is a DVD-RAM.

7. The copyright protection method according to claim 2, wherein said optical disk is a hybrid DVD comprising a RAM area and a ROM area as information storage areas.

8. The copyright protection method according to claim 1, further comprising the steps of:

(d) storing the cryptosystem;

(e) reading the cypher key from the digital recording medium; and

(f) decrypting the encrypted information recorded on the digital recording medium using the cypher key read in step (e).

9. The copyright protection method according to claim 1, wherein said cryptosystem is a modulation method for modulating information to be recorded using a varied table whose relationship between symbols and codes are varied from a predetermined table, and said table identification information representative of the varied table is used as the cypher key.

10. The copyright protection method according to claim 9, wherein said predetermined table is an eight-to-fourteen modulation plus (EFM+) table when the digital recording medium is a DVD.

11. The copyright protection method according to claim 10, wherein said table identification information is a data symbol value in the predetermined EFM+ table corresponding to a data symbol value "0" in the varied EFM+ table.

12. A digital recording medium comprising:

a data recording region on at least a part of which information encrypted using a cryptosystem is recorded; and

a copy disapproval region on which a cypher key for decryption of the encrypted information recorded on the data recording region is recorded.

13. The digital recording medium according to claim 12, wherein said digital recording medium is an optical disk and said cypher key is recorded on a burst cutting area (BCA).

14. The digital recording medium according to claim 13, wherein said cypher key is recorded on a BCA preamble.

15. The digital recording medium according to claim 13, wherein said optical disk is a digital versatile disk (DVD) and said cryptosystem is a content scramble system.

16. The digital recording medium according to claim 13, wherein said optical disk is a DVD-ROM.

17. The digital recording medium according to claim 13, wherein said optical disk is a DVD-RAM.

18. The digital recording medium according to claim 13, wherein said optical disk is a hybrid DVD comprising a RAM area and a ROM area as information storage areas.

19. The digital recording medium according to claim 12, wherein said cryptosystem is a modulation method for modulating information to be recorded using a varied table whose relationship between symbols and codes are varied from a predetermined table, and said table identification information representative of the varied table is used as the cypher key.

20. The digital recording medium according to claim 19, wherein said predetermined table is an eight-to-fourteen modulation plus (EFM+) table when the digital recording medium is a DVD.

21. The digital recording medium according to claim 20, wherein said table identification information is a data symbol value in the predetermined EFM+ table corresponding to a data symbol value "0" in the varied EFM+ table.

22. A playback apparatus for a digital recording medium including a data recording region on at least one part of which information encrypted using a cryptosystem is recorded; and a copy disapproval region on which a cypher key for decryption of the encrypted information recorded on the data recording region is recorded, the playback apparatus comprising:

a memory for storing the cryptosystem;

a reader for reading data recorded on the digital recording medium; and

a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

23. A digital recording and/or reproducing apparatus comprising:

a digital recording medium including a data recording region on at least a part of which information encrypted using a cryptosystem is recorded and a copy disapproval region on which a cypher key necessary for decryption of the encrypted information recorded on the data recording region is recorded;

a memory for storing the cryptosystem;

a reader for reading data recorded on the digital recording medium; and

a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

24. The digital recording and/or reproducing apparatus according to claim 23, wherein said digital recording medium is an optical disk and said cypher key is recorded on a burst cutting area (BCA).

25. The digital recording and/or reproducing apparatus according to claim 24, wherein said cypher key is recorded on a BCA preamble.

26. The digital recording and/or reproducing apparatus according to claim 24, wherein said optical disk is a digital versatile disk (DVD) and said cryptosystem

is a content scramble system.

27. The digital recording and/or reproducing apparatus according to claim 24, wherein said optical disk is a DVD-ROM.

28. The digital recording and/or reproducing apparatus according to claim 24, wherein said optical disk is a DVD-RAM.

29. The digital recording and/or reproducing apparatus according to claim 24, wherein said optical disk is a hybrid DVD comprising a RAM area and a ROM area as information storage areas.

ABSTRACT OF THE DISCLOSURE

A digital recording medium for protecting a copyright includes a data recording region on at least a part of which information encrypted using a cryptosystem is recorded, and a copy disapproval region on which a cypher key for decryption of the encrypted information recorded on the data recording region is recorded. When the digital recording medium is copied illegally, table identification information recorded thereon will be damaged. Thus, the information recorded on a recording medium obtained by illegally copying the digital recording medium cannot be reproduced normally. A playback apparatus for the digital recording medium includes a memory for storing the cryptosystem, a reader for reading data recorded on the digital recording medium, and a decrypter for decrypting the encrypted information recorded on the digital recording medium, based on the cypher key read from the digital recording medium by the reader.

FIG. 1

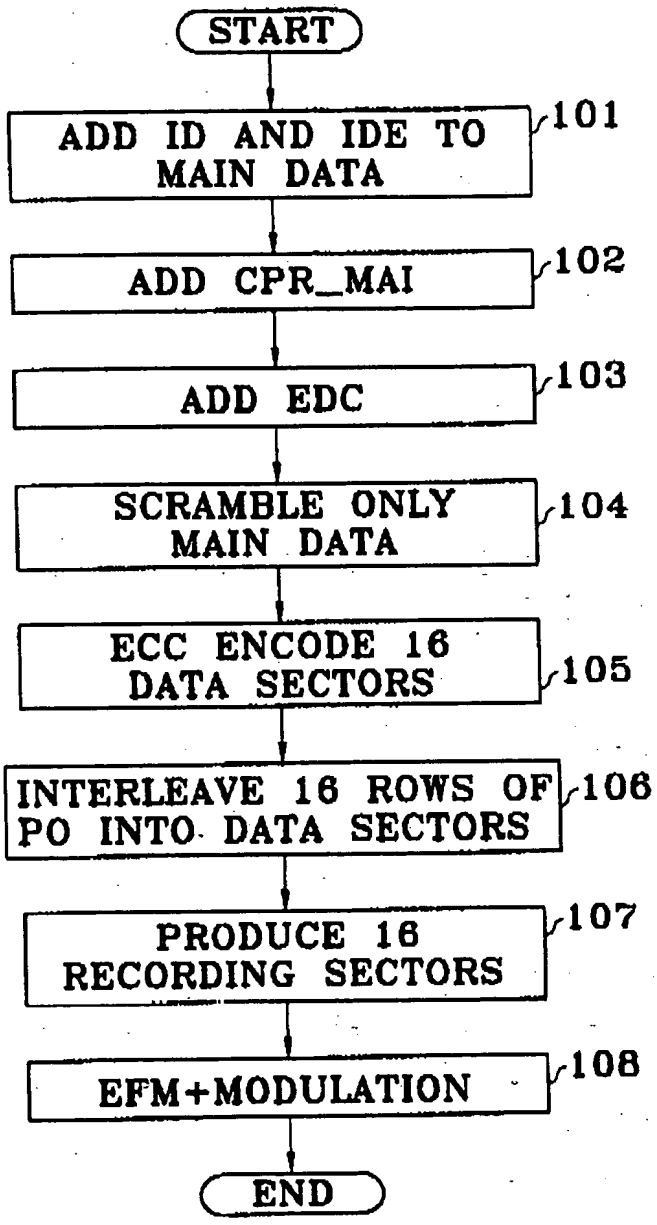


FIG. 2

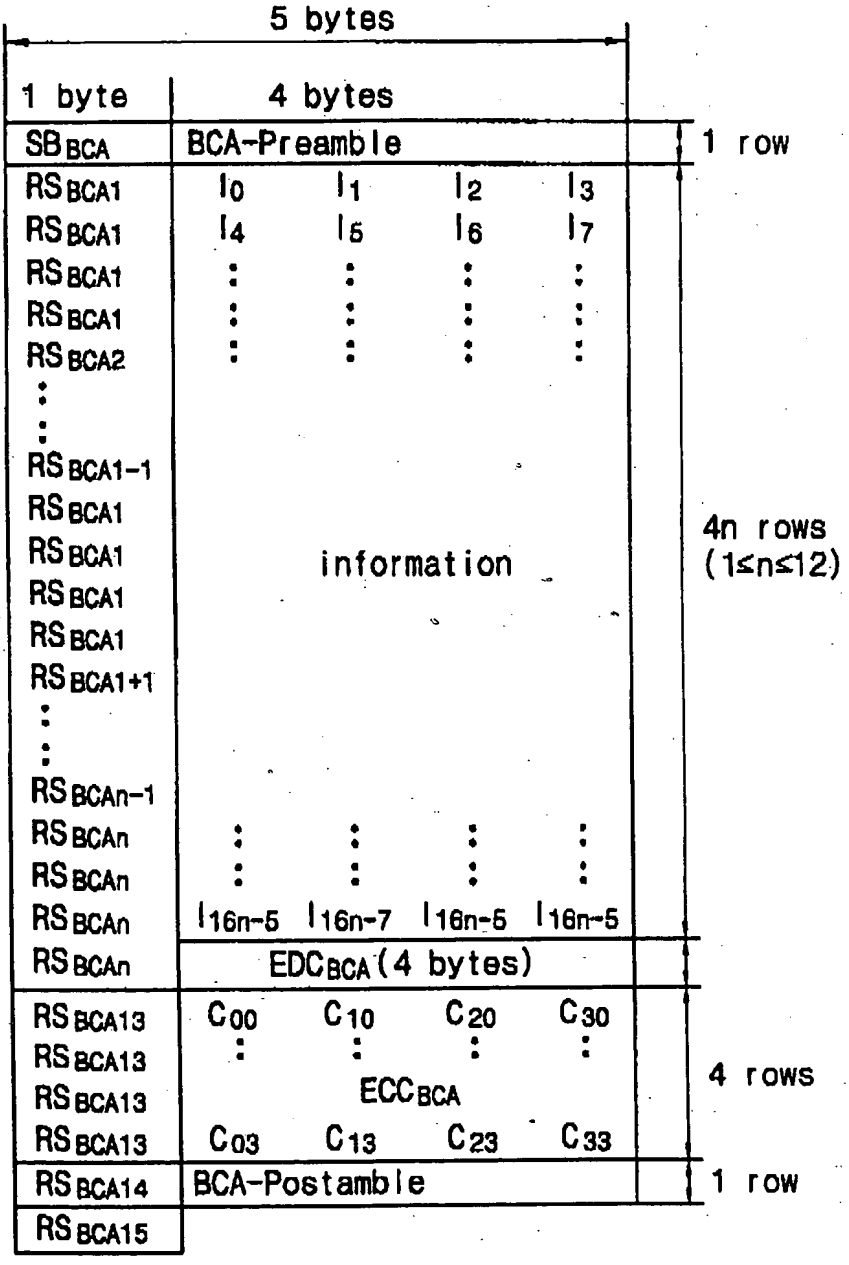

5 bytes
1 byte
4 bytes
SB BCA
BCA-Preamble
1 row
RS BCA1
I0 I1 I2 I3
I4 I5 I6 I7
RS BCA2
RS BCA1-1
information
4n rows
(1≤n≤12)
RS BCAn-1
I16n-5 I16n-7 I16n-5 I16n-5
EDC BCA (4 bytes)
RS BCA13
C00 C10 C20 C30
ECC BCA
C03 C13 C23 C33
4 rows
RS BCA14
BCA-Postamble
1 row
RS BCA15

FIG. 3

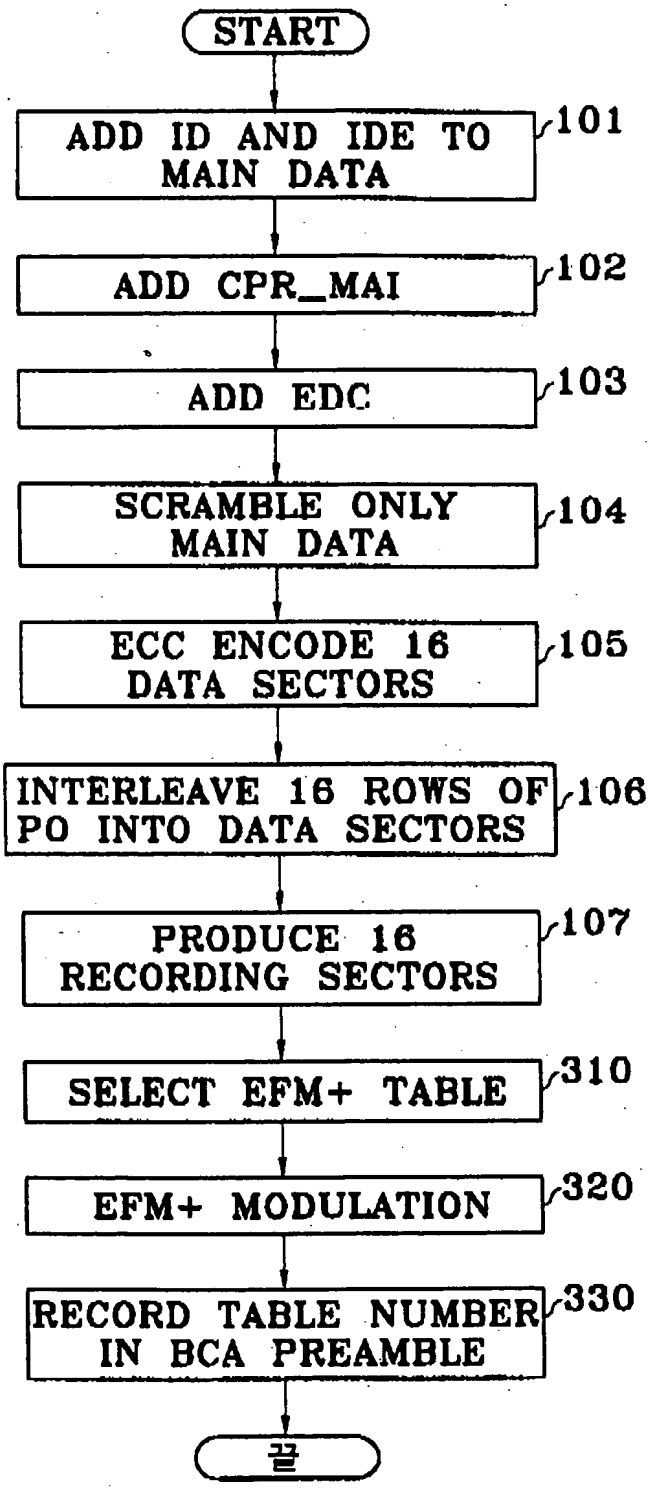
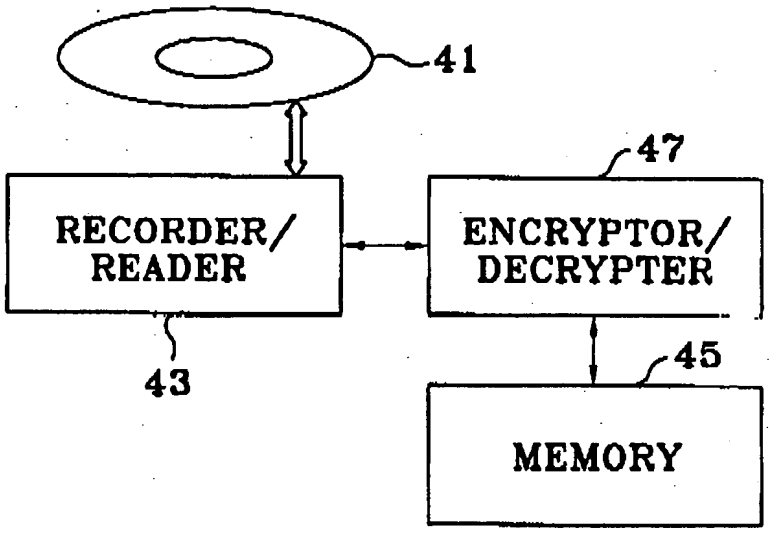

START
ADD ID AND IDE TO MAIN DATA
101
ADD CPR_MAI
102
ADD EDC
103
SCRAMBLE ONLY MAIN DATA
104
ECC ENCODE 16 DATA SECTORS
105
INTERLEAVE 16 ROWS OF PO INTO DATA SECTORS
106
PRODUCE 16 RECORDING SECTORS
107
SELECT EFM+ TABLE
310
EFM+ MODULATION
320
RECORD TABLE NUMBER IN BCA PREAMBLE
330
끝

FIG. 4



中華民國專利公報 [19] [12]

[11]公告編號：408290
[44]中華民國 89年 (2000) 10月11日
發明 全 5 頁

[51] Int.Cl 06: G09C1/00

[54]名 稱：用以保護數位化記錄媒體著作權之方法與裝置以及受著作權保護之數位化記錄媒體

[21]申請案號：087121814 [22]申請日期：中華民國 87年 (1998) 12月29日

[72]發明人：
金秉俊 韓國
[71]申請人：
三星電子股份有限公司 韓國
[74]代理人：羅炳榮 先生

1

[57]申請專利範圍：

1.一種用以保護有關數位化記錄媒體之著作權的著作權保護方法，該著作權保護方法包括下列各步驟：

(a)使用一種密碼系統對待記錄的資訊予以加密；

(b)將步驟 (a)所加密的資訊記錄到數位化記錄媒體上；和

(c)利用一種禁止對密碼鑰拷貝的方式，將這密碼鑰記錄到數位化記錄媒體上，以便對步驟 (a)所加密的資訊予以解密。

2.如申請專利範圍第 1項所述之著作權保護方法，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區 (burst cutting area，BCA)。

3.如申請專利範圍第 2項所述之著作權保護方法，其中所述之密碼鑰是被記錄在

2

— BCA 前同步訊號上。，

4.如申請專利範圍第 2項所述之著作權保護方法，其中所述之光碟片是一種數位

5. 化多用途光碟片 (DVD)，而所述之密碼系統則是一種內容編密系統。

5.如申請專利範圍第 2項所述之著作權保護方法，其中所述之光碟片是一種 DVD-ROM。

10. 6.如申請專利範圍第 2項所述之著作權保護方法，其中所述之光碟片是一種 DVD-RAM。

7.如申請專利範圍第 2項所述之著作權保護方法，其中所述之光碟片是一種混合

15. DVD，其包括一 RAM區和一 ROM區作為資訊儲存區。

8.如申請專利範圍第 1項所述之著作權保護方法，進一步包括下列各步驟：

(d)對密碼系統加以儲存；

3

(e)從數位化記錄媒體讀取密碼鑰；和

(f)使用步驟(e)所讀取的密碼鑰對數位化記錄媒體所記錄的加密資訊予以解密。

9.如申請專利範圍第1項所述之著作權保護方法，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。

10.如申請專利範圍第9項所述之著作權保護方法，其中當數位化記錄媒體為DVD時，所述之預定表即為一個八轉十四調變正數(EFM+)表。

11.如申請專利範圍第10項所述之著作權保護方法，其中所述之表識別資訊是預定EFM +表中與變體EFM+表中資料符號數值「0」對應的一個資料符號數值。

12.一種數位化記錄媒體，其包括：

一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和

一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之如密資訊予以解密的密碼鑰。

13.如申請專利範圍第12項所述之數位化記錄媒體，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區(burst cutting area，BCA)。

14.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之密碼鑰是被記錄在一BCA前同步訊號上。

15.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種數位化多用途光碟片(DVD)，而所述之密碼系統則是一種內容編密系統。

16.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一

4

種DVD-ROM。

17.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種DVD-RAM。

18.如申請專利範圍第13項所述之數位化記錄媒體，其中所述之光碟片是一種混合DVD，其包括一RAM區和一ROM區作為資訊儲存區。

19.如申請專利範圍第12項所述之數位化記錄媒體，其中所述之密碼系統是以一種將一預定表的符號和代碼字之間關係加以變更的變體表，以供調變待記錄資訊的調變方法，而代表該變體表的表識別資訊則用來作為密碼鑰。

20.如申請專利範圍第19項所述之數位化記錄媒體，其中當數位化記錄媒體為DVD時，所述之預定表即為一個八轉十四調變正數(EFM+)表。

21.如申請專利範圍第20項所述之數位化記錄媒體，其中所述之表識別資訊是預定EFM +表中與變體EFM+表中資料符號數值「0」對應的一個資料符號數值。

22.一種數位化記錄媒體的重放裝置，該媒體包括一資料記錄區域，其上至少有一部份係記錄使用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之如密資訊予以解密的密碼鑰，該重放裝置則包括：

一記憶體，用以儲存密碼系統；

一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和

一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

23.一種數位化記錄和／或重製裝置，其包括：

一數位化記錄媒體，該媒體包括一資料記錄區域，其上至少有一部份係記錄使

5

用某種密碼系統予以加密的資訊；和一禁止拷貝區域，其上係記錄對資料記錄區域所記錄之加密資訊予以解密的密碼鑰；

一記憶體，用以儲存密碼系統；

一讀取器，用以讀取數位化記錄媒體上所記錄的資料；和

一解密器，可根據讀取器從數位化記錄媒體所讀取的密碼鑰而對數位化記錄媒體上所記錄的加密資訊予以解密。

24.如申請專利範圍第23項所述之數位化記錄和／或重製裝置，其中所述之數位化記錄媒體是一片光碟片，而所述之密碼鑰則被記錄在一叢發切割區 (burst cutting area， BCA) 。

25.如申請專利範圍第24項所述之數位化記錄和／或重製裝置，其中所述之密碼鑰是被記錄在一 BCA前同步訊號上。

26.如申請專利範圍第24項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種數位化多用途光碟片 (DVD)，而所述之密碼系統則是一種內容編密系統。

6

27.如申請專利範圍第24項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種 DVD-ROM。

28.如申請專利範圍第24項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種 DVD-RAM。

29.如申請專利範圍第24項所述之數位化記錄和／或重製裝置，其中所述之光碟片是一種混合 DVD，其包括一 RAM區和一 ROM區作為資訊儲存區。

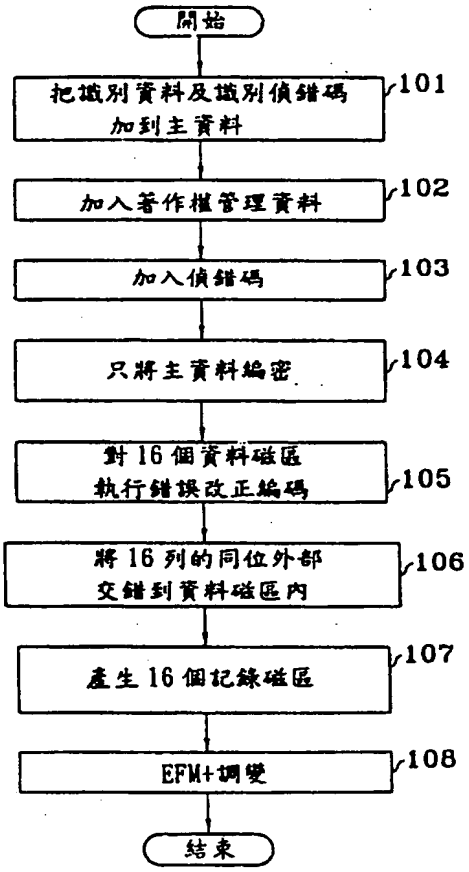
圖式簡單說明：

第一圖為一流程圖，係用以解釋 DVD-ROM上記錄有資料時的訊號處理情形；

第二圖係顯示一種 BCA碼的結構；

第三圖為一流程圖，係用以解釋依據本發明其中之一實施例所構成之 DVD-ROM上記錄有資料時的訊號處理情形；和

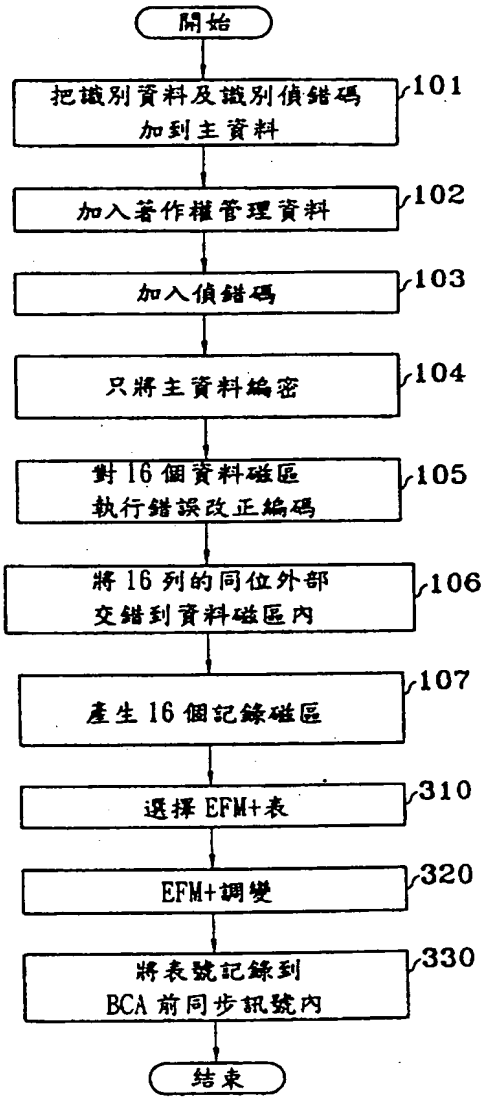
第四圖為一方塊圖，顯示出依據本發明另一實施例所構成的一種數位化記錄／重製裝置。



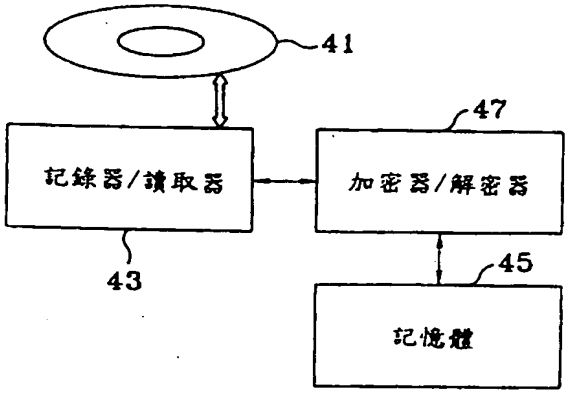
第 圖

	5 bytes				
1 byte	4 bytes				
SB_{BCA}	BCA-前同步訊號				1 列
RS_{BCA1}	I_0	I_1	I_2	I_3	
RS_{BCA1}	I_4	I_5	I_6	I_7	
RS_{BCA1}	:	:	:	:	
RS_{BCA1}	:	:	:	:	
RS_{BCA2}	:	:	:	:	
:					
RS_{BCA1-1}					
RS_{BCA1}					
RS_{BCA1}	資訊				4n 列 (1≤n≤12)
RS_{BCA1}					
RS_{BCA1}					
RS_{BCA1+1}					
:					
RS_{BCAn-1}					
RS_{BCAn}	:	:	:	:	
RS_{BCAn}	:	:	:	:	
RS_{BCAn}	I_{16n-5}	I_{16n-7}	I_{16n-5}	I_{16n-5}	
RS_{BCAn}	EDC_{BCA} (4 bytes)				
RS_{BCA13}	C_{00}	C_{10}	C_{20}	C_{30}	
RS_{BCA13}	:	:	:	:	4 列
RS_{BCA13}	ECC_{BCA}				
RS_{BCA13}	C_{03}	C_{13}	C_{23}	C_{33}	
RS_{BCA14}	BCA-後同步訊號				1 列
RS_{BCA15}					

第二圖


開始
把識別資料及識別偵錯碼加到主資料
101
加入著作權管理資料
102
加入偵錯碼
103
只將主資料編密
104
對16個資料磁區執行錯誤改正編碼
105
將16列的同位外部交錯到資料磁區內
106
產生16個記錄磁區
107
選擇EFM+表
310
EFM+調變
320
將表號記錄到BCA前同步訊號內
330
結束

第三圖


41
47
記錄器/讀取器
加密器/解密器
43
45
記憶體

第四圖

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.